

AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

LISTING OF CLAIMS:

1. (original) A multicast delivery system comprising:

a delivery server which enciphers delivery data by using a current use cipher key to generate enciphered data and transmits a multicast packet containing said enciphered data and a current use key identifier indicative of a pair of said current use cipher key and a current use decipher key as current use keys;

a key management server which is connected with said delivery server through a network, holds as a current use key data, a set of said current use decipher key and said current use key identifier, and transmits a set of said current use decipher key and said current use key identifier as a current use decipherment key data in response to a current use key data request; and

a client terminal which is connected with said delivery server and said key management server through said network, receives said multicast packet from said deliver server, issues said current use key data request to said key management server to receive said current use decipherment key data from said key management server, holds said set of said current use decipher

key and said current use key identifier, and deciphers said enciphered data contained in said multicast packet by using said current use decipher key when said current use key identifier contained in said multicast packet is coincident with said current use key identifier held in said client terminal.

2. (original) The multicast delivery system according to claim 1, wherein said delivery server generates and holds as a current use encipherment key data, a set of said current use cipher key, said current use decipher key and said current use key identifier, and transmits a set of said current use decipher key and said current use key identifier as said current use decipherment key data to said key management server, and

said key management server holds said current use decipher key and said current use key identifier as said current use decipherment key data.

3. (original) The multicast delivery system according to claim 2, wherein said delivery server sets a current use key remaining effective time data to said current use key data, and transmits a set of said current use decipher key, said current use key identifier, and said current use key remaining effective time data as said current use decipherment key data to said key management server,

said key management server holds said current use decipherment key data, and

said delivery server, said key management server and

said client terminal decreases said current use key remaining effective time data as time elapses.

4. (original) The multicast delivery system according to claim 3, wherein said delivery server generates as a next use key data, a set of a next use cipher key, a next use decipher key, a next use key identifier indicative of a pair of said next use cipher key and a next use key remaining effective time data, when said current use key remaining effective time data becomes a first present value, and transmits a set of said next use decipher key, said next use key identifier, and said next use key remaining effective time data to said key management server as a next use decipherment key data, and

said key management server holds said next use decipher key data.

5. (original) The multicast delivery system according to claim 4, wherein said client terminal issues a next use key request to said key management server when said current use key remaining effective time data becomes a second present value smaller than said first preset value, and receives and holds said next use decipherment key data from said key management server.

6. (original) The multicast delivery system according to claim 5, wherein said delivery server enciphers said delivery data by using said next use cipher key as said current use cipher key after said current use key remaining effective time data becomes 0.

7. (original) The multicast delivery system according to claim 1, wherein said delivery server issues a current use key data generating request to said key management server,

said key management server generates and holds as a current use key data, a set of said current use cipher key, said current use decipher key and said current use key identifier in response to said current use key data generating request, and transmits a set of said current use cipher key and said current use key identifier as a current use encipherment key data to said delivery server, and

said delivery server holds said current use encipherment key data.

8. (original) The multicast delivery system according to claim 7, wherein said key management server sets a current use key remaining effective time data to said current use key data, and transmits a set of said current use decipher key, said current use key identifier, and said current use key remaining effective time data as said current use encipherment key data to said delivery server,

said delivery server holds said current use encipherment key data, and

said delivery server, said key management server and said client terminal decreases said current use key remaining effective time data as time elapses.

Docket No. 8022-1063
Appln. No. 10/713,455

9. (original) The multicast delivery system according to claim 8, wherein said delivery server issues a next use key data generating request to said key management server, when said current use key remaining effective time data becomes a first present value,

said key management server generates and holds as a next use key data, a set of a next use cipher key, a next use decipher key, a next use key identifier indicative of a pair of said next use cipher key and a next use key remaining effective time data in response to said next use key data generating request, and transmits a set of said next use encipher key, said next use key identifier, and said next use key remaining effective time data to said delivery server as a next use encipherment key data, and

said delivery server holds said next use encipherment key data.

10. (original) The multicast delivery system according to claim 9, wherein said client terminal issues a next use key request to said key management server when said current use key remaining effective time data becomes a second present value smaller than said first preset value, and receives and holds said next use decipherment key data of said next use decipher key, said next use key identifier, and said next use key remaining effective time data from said key management server.

11. (original) The multicast delivery system according to claim 10, wherein said delivery server enciphers said delivery data by using said next use cipher key as said current use cipher key after said current use key remaining effective time data becomes 0.

12. (original) The multicast delivery system according to claim 1, further comprising:

a plurality of said delivery servers; and

a plurality of said client terminals,

wherein each of said plurality of delivery server issues a next use key data generating request to said key management server while using said current use cipher key,

said key management server generates and holds as a next use key data, a set of a next use cipher key, a next use decipher key and a current use key identifier indicative of a pair of said next use cipher key and said next use decipher key in response to said next use key data generating request, and transmits a set of said next use cipher key and said next use key identifier as a next use encipherment key data to said delivery server, and

said delivery server holds said next use encipherment key data.

13. (original) The multicast delivery system according to claim 12, wherein each of said plurality of client terminals issues a next use decipher key request to said key management

server when said client terminal does not hold said current use key identifier contained in said multicast packet,

said key management server transmits a set of said next use decipher key and said next use key identifier to said client terminal as a next use decipherment key data, and

said client terminal holds said next use decipherment key data.

14. (original) The multicast delivery system according to claim 12, wherein each of said plurality of delivery servers issues a key data change previous notice to said plurality of clients,

each of said plurality of client terminals issues a next use decipher key request to said key management server in response to said key data change previous notice,

said key management server transmits a set of said next use decipher key and said next use key identifier to said client terminal as a next use decipherment key data, and

said client terminal holds said next use decipherment key data.

15. (original) The multicast delivery system according to claim 1, further comprising:

a plurality of said delivery servers; and

a plurality of said client terminals,

wherein said key management server comprises:

a master server; and

a plurality of slave servers,

wherein each of said plurality of delivery servers issues a next use key data generating request to said master server while using said current use cipher key,

said master server generates and holds as a next use key data, a set of a next use cipher key, a next use decipher key and a current use key identifier indicative of a pair of said next use cipher key and said next use decipher key in response to said next use key data generating request, transmits a set of said next use cipher key and said next use key identifier as a next use encipherment key data to said delivery server, and transmits a set of said next use decipher key and said next use key identifier as a next use decipherment key data to said plurality of slave servers,

each of said plurality of slave servers holds said next use decipherment key data, and

said delivery server holds said next use encipherment key data.

16. (original) The multicast delivery system according to claim 15, wherein each of said plurality of client terminals issues a next use decipher key request to any of said plurality of slave servers when said client terminal does not hold said current use key identifier contained in said multicast packet,

said slave server transmits said next use decipherment key data to said client terminal, and

said client terminal holds said next use decipherment key data.

17. (original) The multicast delivery system according to claim 15, wherein each of said plurality of delivery servers issues a key data change previous notice to said plurality of clients,

each of said plurality of client terminals issues a next use decipher key request to any of said plurality of slave servers in response to said key data change previous notice,

said slave server transmits said next use decipherment key data to said client terminal, and

said client terminal holds said next use decipherment key data.

18. (original) The multicast delivery system according to claim 1, wherein said key management server detects a data amount of said multicast packets and charges a fee to said client terminal based on said detected data amount.

19. (original) The multicast delivery system according to claim 1, wherein said client terminal issues said key data request to said key management server, and

said key management server detects the number of said key data requests and charges a fee to said client terminal based on said detected number of key data requests.

20-59. (canceled)